WIRELESS
SECURITY CHECKLIST
Version 3, Release 1.3

20 April 2006

Developed by DISA for the DOD

Database Reference Number: ____________________

Database entered by: ______________________Date:________

Technical Q/A by: ________________________Date:________

Final Q/A by: ____________________________Date:________

CAT I: _____

CAT II: _____

CAT III: _____

CAT IV: _____

TOTAL: _____

UNCLASSIFIED

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

This page is intentionally left blank.

TABLE OF CONTENTS

This page is intentionally left blank.

SUMMARY OF CHANGES

GENERAL CHANGES:

- The previous release was Version 3, Release 1.2, dated 03 November 2005
- Added VMS 6 procedures to Section 1.0

This page is intentionally left blank.

1. WIRELESS SECURITY CHECKLIST INSTRUCTIONS

The Wireless Security Checklist is divided into several sections based on wireless technology used. A single reviewer may cover all technologies or they may be divided among several reviewers. The approach on how to distribute sections depends upon the environment at the site under evaluation, the size of the review team, and the technical expertise or focus of particular reviewers. Regardless of how the sections are dispersed, the first step should be to obtain a complete list of specific wireless devices approved for use at this location from the IAO. In light of the newness and speed of changes in this technology area, this information should be collected prior to arrival on site. Use the equipment inventory sheet provided to collect information, make copies as required.

At all SRRs, the *designated SRR team member* will conduct a wireless discovery test. If **Wireless Local Area Network (WLAN)** access points and/or clients are found during the test, a Wireless SRR will be scheduled (if not previously scheduled) and the *designated SRR team member* will conduct all Level 1 checks in Appendix A of the checklist. These checks are critical for immediate mitigation of network level security risks.

If the site indicates that WLAN network devices such as access points, bridges, keyboards, **WLAN** clients, or **WPAN** (Bluetooth) systems are used, a Wireless SRR will be scheduled for the site. In addition, the *designated SRR team member* will perform all the general checks in Section 1 and all the checks in Section 2 of the checklist.

If the site indicates that **cellular / PCS telephones phones** are used at the site, the *designated SRR Team member* will perform all the general checks in Section 1 and the wireless telephone checks in Section 3 of the checklist. These checks consist of interview questions, which are appropriately included in the IAO interview.

If the site indicates that **broadband wireless** network systems are used or cellular data interface cards (3G) are used with laptop computers, the *designated SRR Team member* will perform all the general checks in Section 1 and the Broadband Wireless checks in Section 3 of the checklist.

If the site indicates that **PDAs** are used or **cellular data interface cards (3G) are used with PDAs** at the site, the *SRR Team Lead* will perform all the general checks in Section 1 and the PDA checks in Section 3 of the checklist. These checks are all interview questions, which are appropriately included in the IAO interview. A sample check of 10-25% of the site's PDAs and corresponding workstations where the PDAs are synchronized is required. Note that some PDAs used at the site may never be connected to a wireless network (the Wireless STIG and this checklist also cover non-wireless PDAs

If the site indicates that **two-way pagers and Short Messaging Service (SMS)** are used at the site, the *SRR Team Lead* will perform all the general checks in Section 1 and the two-way pagers and Short Messaging Service (SMS) checks in Section 4 of the checklist. These checks are all interview questions, which are appropriately included in the IAO interview.

If the site indicates that **Blackberry** wireless email devices are used at the site, the *SRR Team Lead* will perform all the general checks in Section 1 and the Blackberry wireless email devices checks in Section 4 of the checklist. Most checks are all interview questions, which are appropriately included in the IAO interview. A sample-check of 10-25% of the site's Blackberry wireless email devices, corresponding workstations where the Blackberry devices are synchronized, and the Blackberry Enterprise Server is also required.

Table 1-1. Wireless Security Checklist Process Matrix

Procedure	Purpose	Follow-up	Applicable Sections
Wireless SRR	Site has reported that Wireless equipment is present and a wireless security review is scheduled. All wireless equipment, as listed by the site are reviewed. The SRR will begin with a wireless discovery test.	Falls under the normal SRR process.	All Sections according to equipment located at the site.
SIPRNet Compliance Validation (SCV)	Wireless discovery test only. Special DISA program responsible for performing discovery tests for wireless devices connected to the SIPRNET.	If wireless LAN devices are discovered, it is determined whether they are conducted to the SIPRNET. Any devices found are disconnected and documented. Any unauthorized, mission required wireless systems found are minimally secured using the Level 1 checks in Appendix A and a follow-up Wireless SRR conducted by a DISA team is scheduled	Appendix A, Level 1 Checks
Wireless Discovery Test	Conducted with every SRR using wireless discovery tool. Discover unapproved WLAN devices in the Enclave. Perform Level1 checks in Appendix A if rouge WLAN devices are discovered.	Schedule follow-up Wireless SRR	Appendix A, Level 1 Checks
Site Periodic Wireless Discovery	Will be performed by the site periodically using wireless discovery tools. Must include tests for 802.11 and Bluetooth protocols.	If unauthorized WLAN or WPAN devices are found, either disconnect these devices or ensure they are secured using the Wireless STIG.	Sections 1 and 2
Gold Disk (future wireless check will be included)	Will be performed by the site periodically using Gold Disk to check for wireless NICs in laptops and PCs only	If unauthorized WLAN devices are found, either discontinue use of these devices or disable the wireless NIC.	Perform Gold Disk procedures.

1.1 VMS PROCEDURES

When conducting an Wireless SRR, the Team Lead and the assigned Reviewer identify security deficiencies, provide data from which to predict the effectiveness of proposed or implemented security measures associated with the wireless system and operating environment. Security Readiness Review (SRR) of a DOD wireless system requires that the results of the SRR be tracked using the VMS database.

The Team Lead begins by completing both the Visit and the Visit Summary forms under the appropriate Organization in VMS. During a site review, Reviewers update findings for a requested set of site assets. Reviewers enter findings in VMS by updating the same compliance status screens used by the site's System Administrators (SAs). For wireless assets, Reviewers will update assets and findings manually using VMS screen rather than an XML script. When the Reviewer is finished updating SRR results associated with each asset, the Team Lead will compile an executive summary, finalize the Visit information screen in VMS, and request visit approval. Following a review, the Team Lead reports the results back to the Director who requested the review. After reviewing the results of the Visit, the Director can then access VMS to provide any required approvals.

1.1.1 Adding an Organization

When Team Leads arrange a visit, if the site does not exist in VMS, a new organization may be requested.

1. Click Organization Maint. in the VMS navigation pane and then click Request to access the Request Organization form.
2. Complete all of the required fields on the form.
3. Click Submit.

1.1.2 Creating a Visit

A visit is a period of time in which the Team Lead/Reviewer validates the IAVM and STIG vulnerability statuses of assets, and produces a report of their findings. During this time, Team Leads perform a variety of visit maintenance tasks in VMS. Team Leads use the Visit Maint. function whenever they need to create a visit. The Create Visit function is used to identify a visit's status, Team Lead, Reviewers, start/end dates and location. Complete the following steps to create a visit.

1. Click Visit Maint. from the VMS Home page.
2. From the Navigation pane, Click the Create Visit folder icon to display the Create Visit form.
3. Complete all required fields on the Location, General and Reviewers tabs.
4. Click Save Changes when finished

1.1.3 Registering and Managing Wireless Assets

In VMS, an asset is defined as a hardware device or an operating system image that hosts an application (or workload) that is accessed by more than one user. An asset may also include physical locations or other non-computing assets, such as a SWLAN or WLAN. Unclassified asset components are registered in VMS via the NIPRNet and confidential or secret asset components are registered via the SIPRNet. The Team Lead or the SA must register assets.

Both the Reviewer and the SA will create, maintain, and track assets in VMS. The reviewer will use the Asset and Finding Maintenance screen to perform these functions. The SA will use the By Location navigation chain to perform the same function. When Reviewers access the Asset and Finding Maintenance screen, the Navigation pane displays a white Visits folder. Expand this Visits folder to display its subfolders. Each subfolder represents an individual visit in VMS that has been assigned for review. Click (+) to expand the visit and display the location summaries for the visit. Within the location wireless assets are tracked using one of the following asset types.

- Computing – Assets which have an OS such as PEDS and network devices and clients.
- Non-Computing – Used for registering wireless networks

Use the following matrix to select the appropriate asset type for each wireless asset. Note that a wireless network is registered as a separate Non-computing asset but the network hardware components must also be registered as Computing assets. Both assets must be included in the SRR of a wireless network to ensure a complete review of all applicable security policies.

Table 1-2. Asset Matrix

Wireless Technology	VMS Asset Type	Asset Posture
Wireless Network (SWLAN, WWAN, WLAN, WPAN)	Non-Computing	Wireless Policy
RFID	Non-Computing	Wireless Policy
Wireless Camera	Computing	Follow procedures for Video Teleconferencing if applicable **Operating System** – Network Device, Embedded OS->Other Network OS **Network:** Wireless -> Wireless Client
WLAN Access Point	Computing	**Operating System** – select one of the following: Cisco IOS, Junos, or Network Device Embedded OS->Other Network OS **Role**: Enclave Infrastructure **Network**: Wireless -> Access Point
WLAN Security Gateway, Router, Bridge, and/or Switch **NOTE**: these devices often combine functionality, including AP services.	Computing	**Operating System** – select one of the following: Cisco IOS or Network Device Embedded OS->Other Network OS **Role**: Enclave Infrastructure **Network**: Select Wireless Switch, then drill down and select all other applicable functionality based on configuration and use of the specific network device at this site. (e.g., Layer 3 Switch, VPN, Router, etc.)
SWLAN Access Points/Bridges	Computing	**Operating System** – Other Network **Role**: Enclave Infrastructure **Network**: Wireless -> Harris SecNet 11 or 54

Wireless Technology	VMS Asset Type	Asset Posture
SWLAN clients (SecNet 11, 54)	Computing	**Application** – Select all that apply (e.g. Browsers, Office Automation, etc). See the VMS procedures for the operating system SRR and the Desktop Checklist for more details. **Role**: Workstation **Network**: Wireless ->Wireless Client **NOTE**: Do not select SecNet 11 or 54, which is only selected for network devices.
WLAN or WWAN (broadband) Network Client (with OS)	Computing	**Operating System** – drill down to OS then further down into service pack or version OS as applicable. **Application** – Select Antivirus and then applicable version installed. **Application** – Select all that apply (e.g. Browsers, Office Automation, etc). See the VMS procedures for the operating system SRR and the Desktop Checklist for more details. **Role -** Workstation **Network -** Wireless Client
PDA with NIC	Computing	**NOTE**: Do not mark as a workstation **Operating System** – Embedded OS->Other Network OS **Application** -> Antivirus. Currently, there are no options for this device **Application** – Currently, there are no options for this device **Role** – Currently, there are no options for this device **Network -** Wireless PDA/PED
PDA without NIC	Computing	**NOTE**: Do not mark as a workstation **NOTE**: Do not enter IP or MAC address **Operating System** – Embedded OS->Other Network OS. **Application** -> Antivirus. Currently, there are no options for this device. **Application** – Currently, there are no options for this device. **Role** – Currently, there are no options for this device **Network -** Wireless -> PDA/PED
Blackberry Enterprise Server **NOTE**: Only configure asset for applications installed on the **same** server as the BES application.	Computing	**Operating System** – Expand Windows. Select version then service pack installed. **Application –** Application -> Blackberry Enterprise Server **Application** – Expand Antivirus and then applicable version installed. **Application** – Other applications installed on same server (e.g. SQL, Exchange, Browsers, Office Automation, etc). See the VMS procedures for the operating system SRR checklist for more information. **Role –** Member Server
Blackberry client devices	Computing	**NOTE**: Do not mark as a workstation **NOTE**: Do not enter IP or MAC address **Operating System** – Embedded OS->Other Network IOS. **Application** -> Antivirus. Currently, there are no options for this device. **Application** – Currently, there are no options for this device. **Role** – Currently, there are no options for this device **Network –** Wireless -> Blackberry Client
Wireless Telephone	Computing	**NOTE**: Do not enter IP or MAC address **Operating System** – Embedded OS->Other Network OS.

Wireless Technology	VMS Asset Type	Asset Posture
		Role – not required **Network -** Wireless -> PDA/PED
Wireless Voice-Over-IP system and Telephone Instrument	Computing	**NOTE**: Do not enter IP or MAC address **Operating System** – Embedded OS->Other Network OS **Application** - Antivirus. Currently, there are no options for this device. **Application** – Currently, there are no options for this device. **Role** – Currently, there are no options for this device **Network –** Telecom -> Telecom - VoIP/VoSIP -> Endpoint/Wireless.
Wireless NIC (Not in a laptop)	N/A	Not required to enter this type of asset in VMS
Wireless readers, keyboards, mice	N/A	Not required to enter this type of asset in VMS. Wireless keyboard and mouse policies are currently associated with the Non-Computing, Wireless Policy condition.

VMS also provides icons to help you identify important review items. For example, the red exclamation point icon, located near the bottom of the navigation tree on the right, identifies an item that must be reviewed. Assets are also listed according to the following categories.

- Must Review – Assets that must be reviewed (also marked with a red exclamation point).
- Reviewed – Site assets modified by the Reviewer
- Not Selected for Review – Other site assets that were not targeted for review

NOTE: If you save changes to assets or findings in the Must Review area, VMS will automatically log those assets as reviewed and move them to the Reviewed area.

The asset icon color in the Navigation pane indicates the severity of an open finding for the asset. The cubes on the right describe what each of the colors signifies.

- Red – CAT I
- Orange CAT II
- Yellow – CAT III
- Light Green CAT IV
- Dark Green – No open or not reviewed items.
- Updating SRR Findings to VMS

1.1.3.1 Creating Wireless Assets

To create a wireless network Non-Computing asset, perform the following steps.

1. Expand Asset Findings Maint.
2. Click Assets/Findings.
3. Reviewer Only: Expand Visits and skip to Step 5.
4. SA only: Expand Location then the required organization. Then skip to Step 7.

5. Reviewer Only: Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review. If the Visit is not visible, you have not been designated at the visit level as a reviewer. See your Team Lead.
6. Reviewer Only: Expand the visit and display the location summaries for the visit.
7. Click the Create icon located next to Non-Computing. The asset form is displayed.
8. Click the General tab and enter information into all required fields
    - Host Name
    - Managed By – use for remote locations being managed.
    - Owner Field – use to register asset to parent or child location.
    - Mac level, Confidentiality, and Use – change or verify default values as required.

NOTE: The Asset Identification tab is not used for Non-Computing assets.

9. Click the Asset Posture tab to add functions to the asset.
    - Expand Non-Computing then Network Policy Requirements
    - Click Wireless Policy (required)
    - Click the >> button to the selected option(s) to the Selected window
    - Click Save

To create a wireless Computing asset, perform the following steps.

1. Expand Asset Findings Maint.
2. Click Assets/Findings.
3. Reviewer Only: Expand Visits and skip to Step 5.
4. SA only: Expand Location then the required organization. Then skip to Step 7.
5. Reviewer Only: Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review. If the Visit is not visible, you have not been designated at the visit level as a reviewer. See your Team Lead.
6. Reviewer Only: Expand the visit and display the location summaries for the visit.
7. Click the Create icon located next to Computing. The asset form is displayed.
8. Click the General tab and enter information into all required fields
    - Host Name
    - Managed By – use for remote locations being managed.
    - Owner Field – use to register asset to parent or child location.
    - Mac level, Confidentiality, and Use – change or verify default values as required.
    - Status – select Online or Offline
    - Workstation – If Yes is selected, then also enter entry for Addtl workstations with this image field. Change to Yes only for laptops and desktops used with wireless NICs, including SecNet 11 and 54 PC cards.

9. Click the Asset Identification tab
    - Enter IP address and click Add
    - Enter the MAC address and then click Add

10. Click the Asset Posture tab. In the Available pane, expand Computing and drill down to select the following functions as indicated in the Table 1.2, Asset Posture Matrix in a previous section of this document.
    - Operating System – drill down to required selection
    - Role – drill down to required selection
    - Network - drill down to required selection
    - Click the >> button to the selected option(s) to the Selected window
    - Click Save

1.1.4 Asset Finding Maintenance

As part of the Wireless SRR, Reviewers enter findings manually into VMS as follows.

1. Expand Asset Findings Maint.
2. Expand Assets/Findings
3. Expand Visits to display its sub-folders. *(Reviewer Only SA will expand Location and proceed to step 6.*
4. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
5. Expand the visit and display the location summaries for the visit.
6. Expand either Computing or Non-Computing depending on the asset type registration.
7. Expand Must Review *(Reviewer Only. SA will not see 'Must Review', but will proceed to step 8.*
8. Expand Asset to Review. Ready to review is colored in RED
9. Expand the asset and then each Vulnerability Key.
10. Update the 'Status' of the vulnerability
11. Identify details on all open vulnerabilities
12. If applicable: Apply the same Status and comments to other assets by using the 'apply to other Findings' pane.

1.1.4.1 Verify All Required Assets are Updated

1. Asset Findings Maint
2. Visits
3. Expand visit
4. Expand CCSD
5. Expand location
6. Expand computing or non-computing as applicable.
7. Expand Must Review. Verify checkmarks are gone from all vulnerabilities, indicating the asset is updated/reviewed.
8. If checkmarks remain from previous step, update findings using the procedures for Updating SRR Findings to VMS procedures given in a previous subsection.

1.1.5 Printing Compliance and Summary Reports

Compliance and summary reports can be helpful in preparing for an SRR or for SAs in tracking and monitoring findings status.

1.1.5.1 VC06 Asset Compliance Report

1. Navigate to the Reports Menu and select the VC06 report.
2. Select to do the report by asset or an by organization as needed
3. Select “open” status
4. Sort on desired fields as required
5. Select the following to Display
    - Finding Comments
    - Finding Long Name
    - Because it’s truncated otherwise
    - Finding Details
    - Vulnerability Discussion

1.1.5.2 VC03 Severity Summary Report

Same steps as above but report will give only the vulnerability numbers which match the criteria selected. Can provide a quick check of status.

1.1.5.3 ASO1 Report

The AS01 report assists the reviewer or SA by quickly identifying the assets at the location the review is being performed. In the section “Looking at Network Assets” is a quick step by step instruction in creating the report. May want to do other reports if your site manages or owns assets that are not located at their site. Check Child Locations if applicable. Navigate to the Reports menu, Select the AS01 Report, and select the desired criteria for the report.

1.1.5.4 VL01 Report

The VL03 report assists the reviewer or SA by quickly identifying the IAVMs that will be identified to the asset when you select the operating system of the asset. Navigate to the Reports menu, Select the VL01 Report, and select the desired criteria for the report.

1.2 SRR Worksheets

1.2.1 General Information

Date of Wireless SRR:_________________________

Network Reviewer			**Phone/Location**		
Previous SRR (circle)	Y N	**Date of Previous SRR**			
Number of Current Open Findings					

Site Information Worksheet

Site Name	
Address	
Phone	

Site Personnel Information Worksheet

Position	Name	Phone Number	Email	Area of Responsibility
SM				
IAM				
NSO				

1.2.2 Wireless Equipment Inventory

WLAN and Wi-Max (BWA) Network Device Worksheet

Number of Devices Operating System Version/ Protocol		Functionality	Accessories/Software	Classified Use?	DAA/CTS A Approval?
#	Model: OS: Protocol:	e.g. Access Points, Bridges, Routers, IDS, and VOIP, VPN appliances, broadband base station, broadband subscriber unit, etc	IDS, antivirus, etc.	U,S,TS,SCI	Y/N

Wireless LAN and Cellular 3G Stations Worksheet

WLAN / 3G NIC		Type of Station or assigned platform	Accessories/Software	Classified Use?	DAA/CTS A Approval?
#	Model, embedded or external, etc	PDA, Notebooks, Desktops, keyboards, etc	IDS, antivirus, etc.	(U,S,TS,SCI)	Y/N

Wireless Telephones, Pagers, and Email Devices

Type of Device		Accessories/Software	Classified Use?	DAA/CTSA Approval?
#	e.g. Cellular or PCS Telephone; 2-Way Pager; SMS Device; Wireless Email device	IDS, antivirus, etc.	(U,S,TS,SCI)	Y/N
Cellular/PCS Telephones				
2-Way Pagers/ SMS Devices				
Wireless Email devices (e.g. Blackberry clients or server)				

PDA Worksheet
(PDA's used for processing government data

PDA		Connectivity	Accessories/Software	Classified Use?	DAA/CTSA Approval?
#	Model	e.g. Standalone; Sync Cable to WLAN or wired LAN client; Wireless NIC; dial-up; or etc.	IDS, antivirus, etc.	(U,S,TS,SCI)	Y/N

PDA		Connectivity	Accessories/Software	Classified Use?	DAA/CTSA Approval?

This page is intentionally left blank.

2. REQUIREMENTS APPLICABLE TO ALL TECHNOLOGIES

Perform the checks in this section for all wireless technologies.

WIR0010 All wireless systems must have DAA approval.

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that all wireless systems are approved by the DAA prior to installation and use for processing DoD information **Note:** This item applies to WLAN devices (access points, routers, bridges, switches, IDS's, firewall, and laptops; wireless mice and keyboards; wireless cellular and satellite telephones; PDAs; wireless Broadband equipment; Bluetooth devices; SMS devices; two-way pagers; and two-way email devices, including Blackberry devices. Procedure: This check should be performed in conjunction with WIR0015. To save time on site, and help facilitate the SRR, prior to arrival at the site, complete the Wireless Inventory Sheet and use this information to research FIPS 140-2 compliance for devices identified. Request a copy of the site's wireless equipment inventory list, which is required in PDI WIR0015. Also, request an electronic copy of the SSAA and DAA/CTTA approval documentation for review. Use the inventory list and approval documents to note specific products by model, specifications, location restrictions, classification levels, etc. for which approval was granted. Finally, verify DAA approval for each product includes wireless services, accessories, operating systems, and applications used with each wireless device. Verify the mission need is still valid. Mark as a CAT II finding if a rogue network device is found which is not documented or of which the site is not aware. This may be marked as a CAT I finding if the reviewer determines that the rogue device presents immediate access to government information.	**Level 1 Check** 2.1 2.2.6.1 2.4 2.5 3.2.3 3.3.5.1 3.3.5.2 4.2.3.2 4.3.1.2 4.4.3.2

Comments:

WIR0010 / CAT I / MAC: 1, 2, 3 | CL: C, S, P | IAC: EBCR-1
PDI Short Description: A wireless system does not have DAA approval.

Open		Not a Finding		Not Reviewed		Not Applicable

WIR0011 Personally owned wireless devices will not be used for processing DOD information

O	NF	NR	NA	Policy	STIG Reference
				Personally owned wireless devices will not be used and users should be trained on this requirement. Procedure: Review policy documents and user agreements to verify that this issue is addressed and users are aware of this prohibition. Note that this check includes any non-DOD owned or approved devices and wireless NICs.	3.4.5.2 4.2.3.2 4.3.1.2 4.4.3.2

Comments:

WIR0011 / CAT III/
PDI Short Description: Personally owned wireless devices are used for processing DOD information.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0015 Maintain a list of wireless devices

O	NF	NR	NA	Policy	STIG Reference
				The IAO will maintain a list of all DAA approved WLAN devices. The list will include access point MAC address; access point IP address; wireless client IP address; wireless client MAC address; wireless channel set for each access point; access point DHCP range; type of encryption enabled; encryption key used; access point SSID; manufacturer, model number, and serial number of wireless equipment; equipment location; and assigned users with telephone numbers. Procedure: Interview IAO and verify existence and contents of the list. Ensure the MAC address, user information, and other data elements listed in the PDI are included. What are the procedures for ensuring the list is updated? List should indicate date of last update. Spot-check several wireless devices on the list for accuracy.	2.1

Comments:

WIR0015 / CAT IV / 1-CSP, 2-CSP, 3-CSP / DCHW-1
PDI Short Description: List of wireless devices used is not available or not updated.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0020 Secure all individual functions of multi-functional devices

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that multi-functional wireless devices, meet the security requirements for both functions. For example, both the cellular phone and PDA sections apply to devices combining the cellular phone and PDA functions. If there are conflicts between security requirements for each function the most stringent requirement will be used. **Note**: Multi-functional devices combined with cameras are also evaluated using the PDA section guidance. 3G cellular telephone devices, which provide communications connectivity for laptops and PDAs are considered multi-functional wireless devices. For 3G cellular/camera devices, the broadband wireless checks are applicable. Procedure: Work with the IAO to identify multi-functional wireless devices approved for use. Use the appropriate sections of this checklist to verify that security standards for both functions are followed. If some functions are not currently addressed, review extension and DAA approval documentation carefully to ensure potential security risks have been analyzed and mitigated. The purpose of this check is to ensure that all functions of the wireless system are evaluated for security issues. The category of this finding will depend on the issues found with the system being evaluated. Mark this as a CAT II finding only if the system is a multifunctional device and, when reviewed using the applicable subsection of this checklist, CAT II vulnerabilities are opened. If only CAT III or lower vulnerabilities are found, then Mark as a CAT III or lower.	3.2.3 4.2.3.2

Comments:
WIR0020 / CAT III / 1-CSP, 2-CSP, 3-CSP / DCPR-1, ECSC-1 **PDI Short Description:** Multi-functional wireless devices do not meet the security requirements for both functions.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0030 Document wireless devices in the SSAA

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that wireless devices that connect directly or indirectly (hotsync) to the network are added to site SSAAs. Procedure: Review the SSAA and verify that any wireless devices that connect using a NIC or devices that hotsync to networked devices are documented. Mark this as a CAT III finding if an SSAA does not exist or is not properly updated. Also mark as a finding if required extensions for all wireless devices, which attach to the network have not been obtained.	2.1 3.2.3 4.2.3.2 4.4.3.2

Comments:
WIR0030 / CAT III / 1-CSP, 2-CSP, 3-CSP / DCPR-1 **PDI Short Description:** An SSAA has not been established or is not properly updated.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0040 OS configuration must comply be STIG compliant

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that all wireless devices, particularly laptops, comply with applicable operating system STIGs. **Note**: Currently, there are no STIGs available for either the Palm or the Windows Pocket PC operating systems. Procedure: Interview IAO. Obtain and copy the applicable SRR results and review for compliance. If SRR results are not available, then sample check a representative number of devices	2.2.1.1 2.2.6.2 3.3.5.2

Comments:
WIR0040 / CAT II / 1-CSP / 2-CSP / 3-CSP / ECWN-1 **PDI Short Description:** OS configuration of wireless devices do not comply with applicable operating system STIG.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0050 Anti-Virus software must be STIG compliant

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that vendor supported, DOD approved, anti-virus software is installed and configured in accordance with the Desktop Application STIG on all wireless devices, particularly laptops and PDAs, and kept up-to-date with the most recent virus definition tables. **Note:** This requirement applies to all laptops, PDAs, and SMS devices. This is an automatic CAT IV finding for sites using wireless two-way pagers since this software is not available for those devices. Procedure: Interview IAO. Verify that laptops and PCs are STIG compliant. Obtain and copy the applicable SRR results and review for compliance. Check sample configuration to ensure compliance including checks for the following: • The anti-virus software is configured to scan automatically upon startup (once daily). • Remote device is configured to update virus signatures every 14 days or less or when the CERT provides an updated virus signature. • The anti-virus software is configured to scan e-mail attachments, web site downloads, and all other files prior to placing them on any Government system. The configuration of the anti-virus software will be in auto-detect, auto-protect, or real time protection • Web browser download protection is enabled (e.g., Norton Anti-Virus has the ability to scan all downloaded files, if checked in the Options tab, under Auto-Protect). Mark this as a CAT I if no anti-virus software is installed or if DoD CERT approved anti-virus software is not used. Mark this as a CAT IV if DoD CERT approved anti-virus software is not installed on wireless two-way pagers	3.3.5.2 3.4.3 4.3.1.2 EN570

Comments:

WIR0050 / CAT I / 1-CSP / 2-CSP / 3-CSP / ECVP-1

PDI Short Description: Approved anti-virus software is available but is not installed on the wireless device or the signature file is not kept up-to-date.

Open		Not a Finding		Not Reviewed		Not Applicable	

3. WLAN AND WPAN TECHNOGIES

PDI’s in this section must be applied to **all** wireless devices implementing either 802.11 or WPAN (Bluetooth) protocols, including PDAs and other devices used with removable wireless cards to periodically connect to the network. Some checks may not be applicable to all technologies/devices depending on classification, memory available and protocols used. Perform all checks in Section 1 before beginning this section. Next perform the checks in Section 2.1. Perform all checks in Section 2.2 for all sites, marking checks as not applicable where appropriate. The checks in Section 2.2 are not just applicable to classified WLAN systems but also include policy checks, which ensure 802.11 an Bluetooth systems do not place classified information at risk.

3.1 Compliance Checks for WLAN and WPAN Devices

WIR0060 WLANs must be compliant with DODD 8100.2

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that WLAN systems are compliant with overall network security architecture, appropriate enclave security requirements, and DODD 8100.2 prior to installation. Procedure: View the network diagram and ensure that the following devices exist: JID, Router with access control lists, application level firewall, NID, DMZ, and Split DNS are present as appropriate. Request a copy of STIG results in each area for review. Verify wireless network is separated from ALL wired network devices using a VPN. If a Network Infrastructure Security SRR is being conducted in conjunction with this review, mark this check as not applicable and add a comment.	2.1

Comments:

WIR0060 / CAT II / 1-CSP / 2-CSP / 3-CSP / DCBP-1, ECWN-1
PDI Short Description: WLAN systems are not compliant with security architecture requirements.

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR0280 WLAN devices used for remote connection via the Internet, must comply with PDA policies

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that if a WLAN device is to be used to access a DOD network via the Internet through a public WLAN/Internet gateway (e.g., airport or hotel “hotspot”), the requirements for PDAs for remote Internet access listed in Section 3.4 of the Wireless STIG and the requirements in the Secure Remote Computing STIG will also be met. Procedure: Work with the IAO to identify WLAN devices approved for remote access using public gateways. Use the appropriate sections of this checklist to verify compliance with PDA security requirements.	2.2.6.2

Comments:

WIR0280 / CAT II / 1-SP / 2-SP / 3-SP / EBPW-1, EBRP-1, EBRU-1
PDI Short Description: WLAN devices used to access a DOD network via the Internet through a public gateway do not comply with PDA requirements.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0070 WLANs outside the US must have US Forces and host nation approval

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that WLAN devices installed outside the United States have been approved by the local US Forces command and /or host nation. Procedure: Users of non-licensed devices that are intended for use Outside United States & Possessions (OUS&P) must submit a DD Form 1494 for host nation coordination/approval. Verify existence of approval documentation signed by US Forces Command and/or host nation representatives. Mark this as a finding if approval documentation signed by either the US Forces Command or host nation representative does not exist or is not available for verification.	2.2.6 2.2.6.1

Comments:

WIR0070 / CAT IV /
PDI Short Description: US Forces command and/or host nation approval was not obtain for WLAN installations.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0075 Perform periodic WLAN/WPAN discovery

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that the organization periodically screens for unauthorized or rouge access points, stations, and bridges. Local security policy will address the frequency by which these screenings should occur. ***NOTE:*** Organizations are required to scan for unauthorized wireless devices, regardless of whether they have a WLAN installed. Procedure: Interview the IAO and obtain answers to the following questions. Are wireless discovery tests being conducted? How often? By whom? Is a log of tests available? What is the site policy? - Cat IV if wireless discovery procedures are not periodically implemented. - Cat III if discovery procedure results are not independently certified by an outside organization (e.g. Periodic SRRs) for Classified systems.	2.2.1.1 (WIR0105) 2.2.6.2

Comments:

WIR0075 / CAT III / 1-CSP / 2-CSP / 3-CSP / ECMT-1, ECMT-2
PDI Short Description: Periodic wireless discovery is not performed.

Open		Not a Finding		Not Reviewed		Not Applicable	

NET0210 Wireless network devices must be physically protected.

O	NF	NR	NA	Policy	STIG Reference
				The NSO will ensure that all network devices (i.e., JIDS, IDS, routers, RAS, NAS, firewalls, etc) will be located in a secure room with limited access. The NSO will have ultimate authority to determine who has access both physically and administratively. **Procedure**: Verify that the physical network components are in a secure environment. Mark as a Finding if communications devices are not stored in a secure location.	2.2.2.2.3 2.2.6.1 2.2.6.2

Comments:

WIR0210 / CAT III/ MAC: 1, 2, 3 | CL: C, S, P | IAC: ECSC-1
Short Name: Network devices are not stored in secure Communications room

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0290 Install WLAN network devices (AP, bridges) in DMZ or VLAN

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure WLAN network devices, such as access points and bridges, are placed in a screened subnet (DMZ) or Virtual LAN (VLAN) and separated from the wired internal network. A VPN concentrator or gateway will be placed between the access point and the local DoD network. Procedure: Verify compliance by inspecting the site network topology diagrams and the firewall interface configurations. Since many network diagrams are not kept up-to-date, have network administrator walk through the connections to verify the accuracy of the diagrams.	**Level 1 Check** 2.2.6.2 2.2.2.2.2

Comments:

WIR0290 / CAT II / 1-SP / 2-SP / 3-SP / ECWN-1
PDI Short Description: WLAN access points and bridges are not installed in an isolated subnet.

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR0260 Use FIPS 140-2 encryption for data at rest

Policy
The IAO will ensure all data at rest is encrypted on all WLAN client devices. Encryption system must be FIPS 140-2 certified. Procedure: Request IAO provide the FIPS certificate or vendor documentation.

Comments:

WIR0260 / CAT II / MAC: 1, 2, 3 | CL: C, S, P | IAC: ECCT-1, ECCT-2, ECWN-1, ECSC-1
PDI Short Description: WLAN does not use FIPS 140-2 compliant encryption.

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR0270 Use FIPS 140-2 VPN (layer 2 or 3 with AES or 3DES) to secure WLAN

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that a FIPS 140-2 compliant VPN (layer 2 or 3 with 3DES or AES) will be used to secure the WLAN system. Procedure: Interview the IAO and verify use of FIPS 140-2 compliant VPN with 3DES or AES. Ask to see the FIPS certificate or vendor documentation. If not used, check for documents showing a waiver was obtained or approval by DAA. If a VPN is used but does not use FIPS 140-2 compliant encryption, then this is a CAT III finding. If a VPN is not used then this is a CAT II finding and also see WIR0290.	2.2.6.2 2.2.2.2.2

Comments:							
WIR0270 / CAT II / 1-SP / 2-SP / 3-SP / ECWN-1 **PDI Short Description:** A FIPS 140-2 compliant VPN is not used to secure the WLAN system.							
Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0300 Use an IDS/IPS to monitor the WLAN

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure IDS (network IDS/IPS or wireless IDS/IPS) is used to monitor the wireless network. Procedure: Interview network administrator and verify compliance by inspecting the site network topology and dataflow diagrams. To comply with this requirement, the site may either place an IDS/IPS sensor on the wired portion of the network or use a wireless IDS/IPS.	**Level 1 Check** 2.2.6.2

Comments:							
WIR0300 / CAT II / 1-CSP / 2-CSP /3-CSP / ECID-1, EBVC-1 **PDI Short Description:** An IDS/IPS is not used to monitor the wireless network.							
Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0320 Disable management ports on WLAN network devices when not in use

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure HTTP, SNMP and other management interfaces on wireless access points and bridges will be turned off after initial configuration. These ports will be turned on only for firmware upgrades as needed. **Note:** If this feature is not available on the device, then the port should be protected using strong, two-factor authentication/password. Procedure: Review access point configuration to see if HTTP and SNMP ports are turned off. Ports may be turned on for limited time for firmware updates but must be turned off after use (per Network Infrastructure Security STIG). Do not mark as a finding if this capability is not available on the lower end device but risk is mitigated though use of password protection is used on the port.	**Level 1 Check** 2.2.2.2.2 2.2.6.2

Comments:

WIR0320 / CAT II / 1-CSP, 2-CSP, 3-CSP / DCPP-1
PDI Short Description: WLAN network management ports remain enabled when not in use.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0230 WLAN must have session time out capability and must be set to 15 minutes or less

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that the WLAN provides a session timeout capability and the timeout is set for 15 minutes or less depending on local security policy Procedures: Review the configuration of the wireless security gateway (e.g. VPN) appliance or other applicable network device to ensure session timeout is set for 15 minutes or less. (Normally, this is not in the access point configuration but is set in the wireless security gateway). This setting can sometimes also be set in the AP but this is not the best method of implementation.	**Level 1 Check** 2.2.6.2

Comments:

WIR0230 / CAT II / 1-CSP / 2-CSP / 3-CSP / ECND-1, ECND-2, ECTM-2, ECWN-1
PDI Short Description: WLAN session timeout is not set to 15 minutes.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0250 Set WLAN AP transmit power to lowest possible to obtain signal strength required

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that the WLAN access point is set to the lowest possible transmit power setting that will meet the required signal strength of the area serviced by the access point. Procedure: Interview IAO and request documentation showing signal strength analysis from site survey activities. If available, use testing equipment or WLAN clients to determine if signal strength is, in the reviewer judgment, excessively outside the required area. Lower end APs will not have this setting available—in this case, the site should locate the APs appropriately to achieve compliance with this requirement.	**Level 1 Check** 2.2.6.2

Comments:

WIR0250 / CAT II / 1-CSP / 2-CSP / 3-CSP / ECTM-2, ECWN-1
PDI Short Description: WLAN AP transmit power is not set to the lowest possible level to obtain required signal strength.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0330 Password protect WLAN AP and bridges

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that a password is required for access to the management console of the WLAN access point or WLAN bridging device and that the password complies with DoD password policies. Procedure: Review access point configuration to see if password access is enabled for access to the management and configuration settings. Mark this PDI as a finding if password access to the management console is not enabled.	**Level 1 Check** 2.2.6.2 2.2.2.2.2 NET0230

Comments:

WIR0330 / CAT I / 1-SP / 2-SP / 3-SP / ECND-1, ECND-2, ECPA-1, IAIA-1
PDI Short Description: WLAN communications devices are not password protected in accordance with DISA requirements.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0080 Use FIPS 140-2 encryption with unclassified Bluetooth WLAN devices

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that WPAN devices (e.g. Bluetooth) are not used to transfer, receive, store, or process DoD information, unless FIPS 140-2 compliant cryptographic modules are used to encrypt the data during transmission. **Note**: Increasingly, products come with Bluetooth enabled by default with no means of disabling the Bluetooth radio. Users should ensure products do not have Bluetooth prior to procurement. Procedure: Interview IAO and DAA to ensure there is a site policy stating that Bluetooth devices are prohibited. Verify that a written policy exists stating that Bluetooth will be disabled on all applicable devices. If Bluetooth protocol is used, request IAO provide FIPS certificate for the encryption module used. **Hint**: There are currently no FIPS compliant security gateways for Bluetooth, thus, if Bluetooth is used this is an automatic finding.	2.1 2.3.1.2

Comments:

WIR0080 / CAT II / 1-SC / 2-SC / 3-SC / ECCT-1 (S), ECCT-2 (C)
PDI Short Description: FIPS 140-2 encryption is not used on Bluetooth enabled devices.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0083 Disable Bluetooth on devices without FIPS 140-2 encryption

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that the Bluetooth capability is removed or disabled from the wireless device if FIPS 140-2 validated cryptographic modules are not used. **Note**: Increasingly, products come with Bluetooth enabled by default with no means of disabling the Bluetooth radio. Users should ensure products do not have Bluetooth prior to procurement. Procedure: Review **written** policy or check configuration of a sampling of WLAN/WPAN devices. **Hint**: There are currently no FIPS compliant security gateways for Bluetooth, thus, if Bluetooth is used this is an automatic finding. Mark this as a finding if policy documents are not available or if users are not trained on this requirement.	2.3.1.2

Comments:

WIR0083 / CAT III / 1-S / 2-S / 3-S / ECCT-1 (S)
PDI Short Description: FIPS 140-2 encryption is not used but Bluetooth is enabled.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0240 Use DOD PKI certificates to protect unclassified WLANs

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that PKI certificates are used for identification and authentication of the user on unclassified WLAN systems. Procedure: Interview the IAO and verify use of DOD PKI certificates. Review written policies and training materials. If PKI is not yet implemented on DISANET for this site, so state and mark as “not a finding”.	**Level 1 Check** 2.2.6.2

Comments:

WIR0240 / CAT II / 1-S / 2-S / 3-S / IAIA-1, DCBP-1
PDI Short Description: Unclassified WLAN does not use DoD PKI certificates.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0090 Password protect folders and files on WLAN devices

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that password protection and encryption mechanisms will be placed on folders and files on all 802.11-enabled devices. **Note:** A DISA approved file encryption tool may not be available for a specific wireless device or operating system. Procedure: Review site policy and where possible, work with the IAO to sample check files and folders are password protected by accessing a WLAN station. For classified systems, verify that access and changes to data are recorded in transaction logs that are reviewed periodically or immediately upon system security events. Users are notified of time and date of the last change in data content.	2.2.1.1 2.2.6.2

Comments:
WIR0090 / CAT II / 1-CS / 2-CS / 3-CS / ECCD-1, ECCD-2, ECCR-1, ECCR-2, ECCR-3 **PDI Short Description:** Folders and files on WLAN devices are not password protected.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0100 802.11-enabled devices must have a DISA compliant personal firewall

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that a personal firewall is implemented on each 802.11-enabled wireless device. Procedure: Interview users to verify compliance. Review results of Operating System SRR, if available. Configuration must comply with Desktop STIG settings. Work with NSO and IAO to review configuration of each applicable device. Software or operation system should prevent users from altering software settings. However, if this feature is not available, then obtain copies of user training to determine compliance.	2.2.6.2

Comments:
WIR0100 / CAT III / 1-C / 2-C / 3-SP / DCAT-1, DCAT-2 **PDI Short Description:** A personal firewall is not configured or not used.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0110 Power off WLAN receivers and transmitters when not in use

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that infrared WLAN receivers and transmitters are disabled when not required. The local CTTA should be consulted to determine appropriate methods for disabling a specific Infrared wireless device. Procedure: Review **written** policy and check configuration files of infrared access points. Some access points may have this capability but if the capability is not authorized for use the functionality must be disabled in the configuration or by a method authorized by the CTTA. Use of tape or other blocking method is acceptable.	2.2.2.1.1

Comments:
WIR0110 / CAT IV / 1-CSP / 2-CSP / 3-CSP / ECWN-1 **PDI Short Description:** WLAN receivers and transmitters remain powered on when not in use.

Open		Not a Finding		Not Reviewed		Not Applicable

WIR0125 Enable mutual authentication for peer-to-peer WLANs

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that mutual authentication between each station on the peer-to-peer network occurs before data is transmitted between stations. Procedure: Review any 802.11 or Bluetooth devices used. Client devices that permit peer-to-peer communications should have the "require mutual authentication" setting enabled. Have the SA demonstrate this setting and the authentication method in the wireless NIC's management software. Mark this as a finding if this setting is not enabled or not available.	2.2.2.2.2

Comments:
WIR0125 / CAT II **PDI Short Description:** Mutual authentication is not enabled for peer-to-peer WLAN communication.

Open		Not a Finding		Not Reviewed		Not Applicable

WIR0130 For peer-to-peer WLANs, do not use NICs that cannot be disabled

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that WLAN Network Interface Cards (NICs) that do not have the capability to disable peer-to-peer WLAN communications will not be used. Procedure: Check each model of NIC to determine if peer-to-peer communications can be disabled in the management software. Alternatively, the SA may provide a copy of documentation showing that this feature is available in all NICs authorized for used for connectivity to the WLAN. Mark this as a finding if NICs used do not have this feature.	2.2.2.2.2

Comments:

WIR0130 / CAT III / 1-CSP / 2-CSP / 3-CSP / ECWN-1
PDI Short Description: WLAN NICs without the capability to disable peer-to-peer WLAN communications are in use.

Open		Not a Finding		Not Reviewed		Not Applicable

WIR0140 Change default SSID

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that SSIDs will be changed from the manufacturer's default to a pseudo random word consisting of a combination of characters, numbers, and special characters. If possible, the new SSID should follow DoD network password rules. Procedure: Interview the Network Administrator and review password configuration files to ensure compliance. See Network Infrastructure Security STIG, Appendix C for applicable password standards. This is a network communications device, thus passwords should be recorded and stored in accordance with local procedures. Review the configuration of at least one wireless access point at the site to verify compliance.	2.2.3.1 2.2.6.2

Comments:

WIR0140 / CAT III / 1-CSP / 2-CSP / 3-CSP / IAIA-1 (S), IAIA-2 (C), ECWN-1 (CSP)
PDI Short Description: SSIDs on WLAN access points are set to the manufacturer's default.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0150 Disable SSID broadcast mode

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that the SSID broadcast mode is disabled. WLAN access points that do not allow the SSID broadcast mode to be disabled will not be used. Procedure: Review the configuration of the WLAN access points to verify SSID broadcast is disabled. You may also use a discovery tool or a WLAN client to see if the SSID appears in the SSID list.	2.2.3.1 2.2.6.2

Comments:
WIR0150 / CAT III / 1-CSP / 2-CSP / 3-CSP / ECWN-1 **PDI Short Description:** SSID broadcast mode is not disabled.

Open				Not Reviewed		Not Applicable	

WIR0160 Enable MAC address filtering

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that MAC address filtering is enabled at each access point. **Note:** MAC address filtering may not be practical for large WLAN implementations, unless the WLAN management system allows for MAC distribution lists to be centralized and automatically distributed to the point of authentication. Procedure: Review the configuration of the WLAN access point to check for compliance.	**Level 1 Check** 2.2.3.2 2.2.6.2

Comments:
WIR0160 / CAT II / 1-CSP / 2-CSP / 3-CSP / ECWN-1 **PDI Short Description:** MAC address filtering is not enabled on all access points.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0163 Disable Windows Zero Configuration (WZC) service on the WLAN client

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that the Windows (XP and 2000) WZC service is disabled in any Windows computer that will be used on a wireless LAN. This setting should be verified whenever new software or Windows update are installed on the computer. **Note**: (See configuration procedures in Appendix B). Procedure: For clients with Windows 2000 and Windows XP, check the Windows Services applet to verify that WZC is disabled on WLAN stations.	2.2.5

Comments:

WIR0163 / CAT III / 1-CSP / 2-CSP / 3-CSP / ECWN-1
PDI Short Description: WZC service is not disabled on Windows WLAN stations.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0164 Use WLAN drivers and management utilities that work without WZC service

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that only WLAN drivers and WLAN management software from third party sources that do not depend on the Windows WZC service are used in Windows XP or 2000 computers. (Check with WLAN vendor prior to purchasing equipment.) **Note:** The Windows XP or 2000 WZC service may not be used to manage WLAN connections to the computer. Instead, the WLAN software that is usually provided by the WLAN interface card vendor should be installed and used. Procedure: For clients with Windows 2000 and Windows XP, check the Windows Services applet to verify that WZC is disabled on WLAN stations.	2.2.5

Comments:

WIR0164 / CAT III / 1-CSP / 2-CSP / 3-CSP / ECWN-1
PDI Short Description: WLAN drivers and management software requires Windows WZC service to operate.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0165 Remove WLAN NICs from Windows stations when not in use

O	NF	NR	NA	Policy	STIG Reference

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that WLAN users with Windows XP or 2000 computers remove the WLAN NIC whenever wireless service is not being used. **Note:** This check ensures that the wireless NIC does not become inadvertently enable by the OS or other software during the boot sequence. A few products cannot be permanently disabled and should not be procured for use in a government environment. Procedure: Interview the IAO and request copies of the security training briefing to verify that personnel have been properly instructed in this requirement. WLAN NICs should be removed when wireless network connectivity is either temporarily or permanently not used.	2.2.5

Comments:							
WIR0165 / CAT III / 1-CSP / 2-CSP / 3-CSP / ECWN-1 **PDI Short Description:** WLAN NICs are not removed from Windows XP and 2000 WLAN stations when not in use							
Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0166 Embedded WLAN NICs should not require Windows WZC to operate

O	NF	NR	NA	Policy	STIG Reference
				Prior to purchasing Windows stations with embedded WLAN NICs, the IAO will ensure the station is tested and the following is verified: - The embedded or installed NIC will work with the Windows WZC service disabled. - WLAN management software is available for the WLAN station that does not depend on the Windows WZC service. Procedure: Have IAO demonstrate that WZC is disabled on WLAN stations running Windows. The wireless NIC management utility must have the capability. View the configuration of the NIC management software to ensure a setting to set the radio to OFF is available. Review at least one WLAN client of each model/configuration used by the site to verify that the NIC works with the Windows WZC service disabled. Mark this as a finding if the wireless NIC fails when the Windows WZC service is disabled. Mark this as a finding if WLAN management software is unavailable, not installed on all laptops, or if the software does not work when the Windows WZC service is disabled.	2.2.5

Comments:

WIR0166 / CAT III / 1-CSP / 2-CSP / 3-CSP / ECWN-1
PDI Short Description: Windows stations with embedded WLAN NICs require Windows WZC to operate.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0167 Change default setting for WLAN NIC radio to “Off”

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that laptops with embedded WLAN cards will have the WLAN card radio set to OFF as the default setting. Procedure: Have the IAO demonstrate the configuration of the WLAN card in the NIC management utility. Observe that the card is set to off by default upon startup of the operating system. Verify this is standard practice by sample checking 10% of laptops. Laptops can be checked by verifying the status of the embedded wireless NIC upon boot-up in each profile used on the laptop. This PDI only applies to the embedded WLAN card. The user should be able to enable and disable the NIC in accordance with site policy. Mark as a finding if the embedded NIC radio functionality (transmit or receive setting) is enabled upon system boot or this function cannot be set to default of OFF.	2.2.5

Comments:							
WIR0167 / CAT III / 1-CSP / 2-CSP / 3-CSP / ECWN-1 **PDI Short Description:** Embedded WLAN NICs do not have the radio set to “Off” by default.							
Open		Not a Finding		Not Reviewed		Not Applicable	

3.2 Wireless Keyboards and Mice

Wireless mice must be approved by the DAA and documented in the list of wireless equipment are included in the check for wireless devices in PDI WIR0010. Since wireless mice transmit telemetry data (right, left, etc.), they pose little to no security risk to DOD.

WIR0132 Wireless keyboards must comply with all applicable WLAN requirements

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that laptops with embedded WLAN cards will have the WLAN card radio set to OFF as the default setting. Procedure: Have the IAO demonstrate the configuration of the WLAN card in the NIC management utility. Observe that the card is set to off by default upon startup of the operating system. Verify this is standard practice by sample checking 10% of laptops. Laptops can be checked by verifying the status of the embedded wireless NIC upon boot-up in each profile used on the laptop. This PDI only applies to the embedded WLAN card. The user should be able to enable and disable the NIC in accordance with site policy. Mark as a finding if the embedded NIC radio functionality (transmit or receive setting) is enabled upon system boot or this function cannot be set to default of OFF.	2.4

Comments:

WIR0132 / CAT II / 1-SP / 2-SP / 3-SP / ECWN-1
PDI Short Description: Wireless keyboard do not comply with DISA standards.

Open		Not a Finding		Not Reviewed		Not Applicable	

3.3 Voice-over-IP

WIR0133 Wireless VoIP systems must comply with applicable requirements

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that if wireless keyboards are used, applicable requirements listed in the Wireless STIG, Sections 2.2.6 and 2.3 are followed. Procedure: This procedure depends on the transmission protocol, 802.11 or Bluetooth, used by the keyboard. Annotate the specific issues found in the Comments section. For **all** wireless keyboards, perform these checks from Section 1.0: WIR0010 (DAA approved), WIR0011 (host nation approval), WIR0015 (track on equipment list), WIR0040 (in SSAA). For **802.11** keyboards perform these checks from Section 2.4: WIR0170 (no TS, SCI), WIR0180 (not in SCIFs), and WIR0190 (no classified). For **Bluetooth** wireless devices perform the checks in Section 2.2 and 2.4: (WIR0080 requiring FIPS 140-2 cert. for unclassified usage), (WIR0181 (no classified), and WIR0182 (not in SCIF). **Hint**: This is an automatic CAT II finding if Bluetooth keyboards are used, since FIPS compliant encryption is not yet available for Bluetooth. However, downgrade to a CAT III if any form of encryption is used. Mark as a finding if any CAT I or II checks in Sections 1.0 or 2.0 are marked as a finding.	2.5

Comments:

WIR0133 / CAT II / 1-SP / 2-SP / 3-SP / ECBI-1, ECWN-1
PDI Short Description: Wireless VoIP systems do not comply with DISA standards.

Open		Not a Finding		Not Reviewed		Not Applicable	

3.4 Mitigating Risks to Classified Information

The checks in Section 2.4 apply to all sites that process classified and use WLAN or WPAN devices, regardless of the classification level of the wireless devices. Although a site may not use wireless devices for processing classified, the reviewer must perform checks to verify that policies and procedures exist to prevent or mitigate risk to SCIFs and other areas where classified processing takes place.

WIR0170 Do not use WLAN devices to access TS and SCI information

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that WLAN devices are not used to transfer, receive, store, or process classified information categorized as SCI and TS. Procedure: Interview the IAO and request copies of the security briefing to verify that personnel have been properly instructed in the requirement. Mark this as a finding if WLAN devices are used for classified information or SCI level traffic.	**Level 1 Check** 2.2.6.1

Comments:							
WIR0170 / CAT II / 1-C / 2-C / 3-C / DCSR-3, ECWN-1 **PDI Short Description:** WLAN devices are used to access TS and SCI information.							
Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0180 Do not allow WLAN devices in SCIFs

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that WLAN devices are not permitted in any SCIF. Procedure: Interview the IAO and review site SCIF policies. Request copies of the security briefing to verify that personnel have been properly instructed in the requirement.	2.2.6.1

Comments:							
WIR0180 / CAT II / 1-C / 2-C / 3-C / ECTC-1, ECWN-1 **PDI Short Description:** WLAN devices are allowed to enter or are used in SCIFs.							
Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0181 Disable RF and IR on WPAN devices (e.g. Bluetooth) if allowed into SCIFs

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that no Bluetooth devices are permitted in a permanent, temporary, or mobile SCIF unless the transmit capability (RF and IR) is rendered completely inoperable. Procedure: Review written policies and training material. Powering off is not necessarily effective for all models. Removal of batteries is a more acceptable procedure.	2.3.1.1

Comments:

WIR0181 / CAT II / 1-C / 2-C / 3-C / ECTC-1, ECWN-1
PDI Short Description: WPAN devices are permitted in SCIFed areas.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0182 Bluetooth devices cannot be used to process classified

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that Bluetooth devices are not used to send, receive, store, or process classified messages. Procedure: Interview the IAO and request copies of the security briefing to verify that personnel have been properly instructed in the requirement. Mark this as a finding if bluetooth wireless is used for classified information or SCI level traffic.	2.2.6.1

Comments:

WIR0182 / CAT III / 1-C / 2-C / 3-C / DCSR-3, ECWN-1
PDI Short Description: Bluetooth devices are used to process classified information.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0200 Coordinate with CTTA before installing WLAN devices (SecNet-11) for classified

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that the CTTA has been notified before installation and operation of WLANs intended for use in processing or transmitting classified data, including the SecNet-11. Procedure: Request the IAO provide documents verifying that the CTAA has reviewed the system. Review documentation showing CTTA coordination. Note specific areas identified as approved or prohibited for wireless device use. Review written policies and training material. Verify proper procedures for wireless device use in classified areas is addressed in training program. Mark as a finding if CTTA has not reviewed the system.	2.2.4

Comments:							
WIR0200 / CAT III / 1-C / 2-C / 3-C / ECTC-1 **PDI Short Description:** WLAN devices are installed or used for classified without CTTA approval.							
Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0203 Use NSA Type 1 WLAN devices for transmitting classified

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that only NSA Type 1 certified WLAN systems are used for wireless transmission of classified information. Procedure: Interview the IAO and request copies of the security training briefing to verify that personnel have been properly instructed in the requirement. Mark this PDI as a finding if NSA Type 1 documentation is not available for review. Mark this as a finding if this requirement is not addressed in the site’s classified security training materials.	2.2.6.1

Comments:							
WIR0203 / CAT I / 1-C / 2-C / 3-C / DCSR-3, ECWN-1 **PDI Short Description:** Classified data is transmitted using non-NSA Type 1 certified WLAN systems.							
Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0204 Obtain DSAWG approval for WLAN systems connected to the SIPRNet

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that all WLAN systems connected to the SIPRNet have been approved by the DSAWG. Procedure: Verify that any systems identified as connected to the SIPRNet either through discovery or IAO identification have approval documents signed by a DSAWG representative. Mark this PDI as a finding if documentation showing DSAWG approval is not available.	2.2.6.1

Comments:
WIR0204 / CAT I / 1-C / 2-C / 3-C / DCSR-3, ECWN-1 **PDI Short Description:** WLAN systems are connected to the SIPRNet without DSAWG approval.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0210 Use DOD High Assurance PKI certificates for Secret and Confidential WLANs

O	NF	NR	NA	Policy	STIG Reference
				For WLANs approved by the DAA for processing Secret or Confidential information, the IAO will ensure DOD High Assurance PKI certificates will be used for authentication in compliance with DOD policy. (SecNet 11 does not provide user identification and authentication.) Procedure: Interview the IAO and verify use of the DOD High Assurance PKI Root Certificate Authority.	2.2.6.1

Comments:
WIR0210 / CAT II / 1-C / 2-C / 3-C / IAIA-2, DCBP-1 **PDI Short Description:** DOD High Assurance PKI certificates are not used for authentication on WLANs that process Secret and Confidential information.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0225 Coordinate with CTTA and disable recording for devices used in classified areas

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that WLANs and WPANs are not operated in areas where classified information is electronically stored, processed, or transmitted unless: - The DAA, in consultation with the CTTA, has approved the use of WLANs or WPANs (such as Bluetooth) devices in the area. - The device's voice recording capability is rendered inoperable. - The WLAN is separated from the classified data equipment by a distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented. Procedure: Review documentation showing CTTA coordination and review of the system. Note specific areas identified as approved or prohibited for wireless device use. Document must also specify distance and countermeasure guidelines. Mark this PDI as a finding if written CTTA coordination does not exist for all systems which process or transmit classified data.	**Level 1 Check** 2.2.6.1 2.3.1.1

Comments:							
WIR0225 / CAT II / 1-C / 2-C / 3-C / ECTC-1 **PDI Short Description:** WLAN devices are used or installed in unauthorized areas.							
Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0190 Do not use clients with embedded wireless NICs that are not removable for classified

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure computers with embedded wireless NICs that cannot be removed by the user will not be used to transfer, receive, store, or process classified information. **Note**: At this time, there are no NSA Type 1 certified devices for encrypting Top Secret information. Procedure: Ask the IAO if there are client devices, which process classified information and have wireless NICs. If there are no such devices, then mark this as not applicable. You must inspect a sampling of laptop devices which process classified to verify this by checking network ports and verifying these ports are not wireless NICs buy manually inspecting or looking at the hardware device drivers configuration screens. Request the IAO demonstrate the removal of the NIC from a sampling of the laptops. Ensure the PC is still operational with the card removed. Mark this item as a CAT I finding if you locate computers, which have embedded wireless NICs, which cannot be removed and are being used for classified processing. Mark this item as a CAT II if there are procedures in place to mitigate this risk, such as disabling the driver or card IR port.	2.2.6.1

Comments:

WIR0190 / CAT II / 1-C / 2-C / 3-C / DCSR-3, ECWN-1
PDI Short Description: Computers with embedded wireless NICs that cannot be removed by the user are used to transfer, receive, store, or process classified information.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0193 Laptops with embedded wireless NICs are connected to SIPRNET

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that all laptop computers connected to the SIPRNET do not have an internal wireless NIC. Procedure: Ask the IAO if there are client devices that process classified information and have wireless NICs. If there are no such devices, then mark this as not applicable. You must inspect a sampling of laptop devices which process classified to verify this by checking network ports and verifying these ports are not wireless NICs by manually inspecting or looking at the hardware device drivers configuration screens. Request the IAO demonstrate the removal of the NIC from a sampling of the laptops. Ensure the PC is still operational with the card removed.	2.2.6.1

Comments:							
WIR0193 / CAT II / 1-C / 2-C / 3-C / DCSR-3, ECWN-1 **PDI Short Description:** Laptop computers with embedded wireless NICs are used to connect to the SIPRNET.							
Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0220 Use NSA Type 1 encryption for Secret and Confidential WLANs

O	NF	NR	NA	Policy	STIG Reference
				For WLANs approved by the DAA for processing Secret or Confidential information, file system encryption will be used on all WLAN client devices with an NSA Type 1 certified encryption software or technique. Procedure: Interview the IAO and verify use of file system encryption by inspecting the WLAN client configuration. Note the software or technique used for encryption and, if applicable, request documentation showing that it is NSA and DAA approved.	2.2.6.1

Comments:							
WIR0220 / CAT II / 1-C / 2-C / 3-C / DCNR-1, IAIA-2, IATS-3, IAGA-1 **PDI Short Description:** An NSA Type 1 certified encryption software or technique is not used to protect WLANs processing Secret or Confidential information.							
Open		Not a Finding		Not Reviewed		Not Applicable	

This page intentionally left blank

4. WIRELESS REMOTE ACCESS TCHNOLOGIES

4.1 Wireless Cellular and PCS Telephones

WIR0350 Use NSA Type 1 telephones for classified transmission

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that only NSA approved Type 1 cellular or satellite telephones will be used for classified voice or classified data wireless telephone transmissions. The classification level of information transmitted over the phone will not exceed the classification level approved for the phone. Procedure: Interview the IAO and request copies of the security briefing to verify that personnel have been properly instructed in the requirement.	3.2.3

Comments:

WIR0350 / CAT II / 1-C / 2-C / 3-C / DCSR-3, ECTC-1, ECCM-1, ECTC-1
PDI Short Description: Cellular or satellite telephones that process classified information are not using NSA-approved, Type 1 end-to-end encryption.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0356 Do not allow wireless phones with cameras into classified document processing areas

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that cellular/PCS phones with digital cameras (still and video) are not allowed in any SCIF or other area where classified documents or information is stored, transmitted or processed. Procedure: Review written policies and training material. Powering off, removal of batteries, or blocking IR ports is not acceptable. These devices should not be permitted in a SCIF regardless. Mark this item a finding if a written policy and user training does not address this requirement.	3.2.3 3.4.5.1

Comments:

WIR0356 / CAT II / 1-C / 2-C / 3-C / ECTC-1, ECCM-1, ECTC-1
PDI Short Description: Wireless phones with cameras are allowed into classified areas.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0360 Disable RF and IR on cellular phones when in a SCIF

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that wireless telephones are prohibited in a permanent, temporary, or mobile SCIF unless the transmit capability (RF and IR) is rendered inoperable. Procedure: Interview the IAO and request copies of the security briefing to verify that personnel have been properly instructed in the requirement.	3.2.3

Comments:

WIR0360 / CAT II / 1-C / 2-C / 3-C / DCSR-3, ECTC-1, ECCM-1, ECTC-1
PDI Short Description: RF and IR on cellular phones are not disabled when in a SCIF

Open		Not a Open		Not Reviewed		Not Applicable	

WIR0370 Coordinate with CTTA and do not hotsync wireless phones in classified processing areas

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that cellular phones are allowed or operated in areas where classified discussions or data processing takes place only when: - The DAA, in consultation with the CTTA, has approved that cellular phones can be brought into the facility and/or used in the facility. - The device's voice recording capability is rendered inoperable. - The phones are separated from the classified data equipment a distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented. - Wireless phones are not connected via hotsync to a workstation in a SCIF. Procedure: Interview DAA and IAO. Obtain a copy of any documentation showing CTTA coordination and note specific areas identified as approved or prohibited for wireless device use. Review written policies and training materiel.	3.2.3

Comments:

WIR0370 / CAT II / / 1-C / 2-C / 3-C / DCSR-3, ECTC-1, ECCM-1, ECTC-1, DCPR-1, DCHW-1
PDI Short Description: Wireless telephones are used in unauthorized areas without proper approval.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0371 Wireless phones with cameras must be approved by physical security policies

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure cellular/PCS phones with digital cameras (still and video) are allowed in a DoD facility only if specifically approved by site physical security policies. Procedure: Review site's physical security policy to see how wireless phones with cameras are handled at this site. Mark this as a finding if there is no written physical security policy outlining whether wireless phones with cameras are permitted or prohibited on or in this DoD facility.	3.2.3 3.4.5.2

Comments:							
WIR0371 / CAT III / 1-CS / 2-CS / 3-CS / PEPF-1, PEPF-2 **PDI Short Description:** Wireless phones with cameras are allowed into a DoD facility without written approval.							
Open		Not a Finding		Not Reviewed		Not Applicable	

4.2 Broadband Wireless

4.2.1 Mitigating Risks to Classified Information

WIR0373 Do not use broadband wireless systems for classified

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that broadband wireless systems will not be used to store, process, or transmit classified and/or SCI information. Procedure: Interview the IAO and request copies of the security briefing to verify that personnel have been properly instructed in the requirement. Mark this as a finding if broadband wireless is used for classified information or SCI level traffic.	3.3.5.1

Comments:

WIR0373 / CAT II / 1-C / 2-C / 3-C / DCSR-3, ECWN-1
PDI Short Description: Broadband wireless is used to access TS and SCI information.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0374 Do not permit broadband wireless in a SCIF

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that broadband wireless devices will not be permitted in a permanent, temporary, or mobile Sensitive Compartmented Information Facility (SCIF). Procedure: Interview the IAO and request copies of the security briefing to verify that personnel have been properly instructed in the requirement.	3.3.5.1

Comments:

WIR0374 / CAT II /
PDI Short Description: Broadband wireless is permitted in a SCIF.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0375 Coordinate with CTTA before using broadband wireless in areas with classified

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that broadband wireless systems shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless: - Approved by the DAA in consultation with the CTTA. - The WLAN is separated from the classified data equipment by a distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented. Procedure: Obtain a copy of any documents showing DAA coordination with the CTTA and note specific areas identified as approved or prohibited for wireless device use. Document must also specify distance and countermeasure guidelines. Mark this PDI as a finding if written CTTA coordination does not exist for all broadband wireless systems which process or transmit classified data.	3.3.5.1

Comments:

WIR0375 / CAT II /
PDI Short Description: Broadband wireless is used in unauthorized areas or do not have proper approval.

Open		Not a Finding		Not Reviewed		Not Applicable	

4.2.2 Compliance Checks for Broadband Wireless Devices

WIR0376 Use DoD PKI certificates for I&A in unclassified broadband wireless

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that PKI certificates are used for identification and authentication (I&A) of the user. Procedure: Interview the IAO and verify use of DoD PKI certificates. Review written policies and training materials. If PKI is not yet implemented on DISANET for this site, so state and mark as “not a finding”.	3.3.5.2

Comments:

WIR0376 / CAT II /
PDI Short Description: DoD PKI certificates are not used for unclassified broadband wireless.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0377 Use a FIPS 140-2 VPN (AES or 3DES) to secure broadband wireless systems

O	NF	NR	NA	Policy	STIG Reference
			2	The IAO will ensure that a FIPS 140-2 compliant VPN (Layer 2 or 3 with 3DES or AES) will be used to secure the broadband wireless system. Procedure: Verify use of FIPS 140-2 compliant VPN with Triple-DES or AES. Ask to see the FIPS certificate or vendor documentation. If not used, check for documents showing a waiver was obtained or approval by DAA. If a VPN is used but does not use FIPS 140-2 compliant encryption, then this is a finding.	3.3.5.2

Comments:

WIR0377 / CAT II /
PDI Short Description: A FIPS 140-2 compliant VPN (with 3DES or AES) is not used to secure the broadband wireless system.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0378 Broadband wireless must comply with Secure Remote Computing STIG policies

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that the requirements in the Secure Remote Computing STIG are met. Procedure: Review the results of the Desktop and Network Infrastructure STIG. Review results for securing broadband connections as applicable.	3.3.5.2

Comments:

WIR0378 / CAT III /
PDI Short Description: Broadband wireless systems are not in compliance with applicable Secure Remote Computing STIG requirements.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0379 Use a personal firewall and IDS to protect the broadband wireless station

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that a personal firewall and an intrusion detection system will be implemented on each broadband wireless client device. Procedure: Interview users to verify compliance. Review results of Operating System SRR, if available. Configuration should comply with Desktop STIG settings. Work with NSO and IAO to review configuration of 10% of broadband wireless devices. Software or operation system should prevent users from altering software settings. However, if this feature is not available, then obtain copies of user training to determine compliance.	3.3.5.2

Comments:

WIR0379 / CAT III /
PDI Short Description: A personal firewall or IDS is available for a broadband wireless station but is not used or is not properly configured.

Open		Not a Finding		Not Reviewed		Not Applicable	

4.3 Personal Digital Assistants (PDAs)

4.3.1 Compliance Checks for PDAs

WIR0450 Configure password protection IAW DISA requirements

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that password protection, where a password must be entered in order to access data and applications, will be used on all PDAs. - A password meeting DoD password policies will be used, if this capability is available - The password will be changed at least every 90 days. - The password protection feature will not permit its bypass without zeroing all data stored on the device. - The password protection feature will be enabled at all times. Procedure: Review site PDA password policy and training with IAO. Users should be trained on the above requirements. A backup procedure should be in place in case of data loss if system is mission critical.	3.4.5.2

Comments:

WIR0450 / CAT I /1-CS / 2-CS / 3-CS / ECCD-1, ECCD-2, ECCR-1, ECCR-2, ECCR-3
PDI Short Description: Password protection is not used or permits bypass without zeroing out data.

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR0460 Use encryption to protect data and files on the PDA

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that tools will be used to encrypt data and files on PDAs. Procedure: **This check applies only to unclassified systems. For classified systems, use WIR0425**. Review site policy and PDA configuration documents. Work with the SA or IAO to verify that all PDAs used to process government data use encryption (may be Palm, Windows, or third party) to protect data stored on the device. Third party, Palm or Windows OS. Verify FIPS certified products by reviewing the IAO provided certificate. Mark this as CAT III finding if encryption is used (Palm, Windows, or third party) but it is not FIPS compliant—this software must have DAA approval. Mark this as CAT II finding if no encryption is used.	3.4.5.2

Comments:
WIR0460 / CAT II / **PDI Short Description:** Encryption tools are available for the PDA but are not installed or configured.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0465 Do not download mobile code from non-DOD sources

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that mobile code is not downloaded from non-DOD sources and is downloaded from only trusted DOD sources over assured channels. Procedure: Review site policy and training with IAO. Interview users to ensure they are aware of and comply with this requirement. Spot-check browser configuration of PDA's web browser , if possible.	3.4.5.2

Comments:
WIR0465 / CAT II / **PDI Short Description:** Mobile code is downloaded from non-DoD sources.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0470 Disable IR port on the PDA when not in use

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that PDAs that are used in areas where DOD information is processed: - Have IR ports are disabled when IR transmissions are not being used. - Data exchange via the IR port should be limited to trusted DOD devices. - The local CSA CTTA should be consulted to determine appropriate method for disabling the IR port on the PDA. Procedure: Interview IAO and ask if there is a written site policy and training program which ensures that users are aware of the policy to disable IR ports and the means by which they are to disable the port. Ensure there is documentation showing CTTA approval of the method used by the site. If possible, interview one or two users to ensure they are aware of and comply with this policy. Mark this as a Category II finding if a policy does not exist to ensure users disable IR ports when not in use. Mark this as a Category IV policy if users are not aware of the policy or the CTTA has not been consulted.	3.4.5.2

Comments:

WIR0470 / CAT II /
PDI Short Description: IR ports on PDAs are not disabled when IR transmissions are not being used or data exchange.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0480 PDA hotsyncing of unclassified data must comply with DISA requirements

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that procedures for hotsyncing unclassified information to the PDA include the following: - The IAO will ensure that only DOD-approved synchronization access control software is used - Hotsync management software is only be launched when hotsyncing the PDA and closed as soon as the hotsync operation has been completed, if the software does not require a password before use. - Hotsync management software will not be launched as part of the computer boot-up process, if the software does not require a password before use. - Synchronization access control software is installed on all workstations that have synchronization software installed on them, if available. - The user disables wireless operations when a PDA is connected to the DISA wired network via a hotsync or other interface cable. - PDAs that transfer, receive, store, process DoD information will not be synced to home or personally owned PCs. Procedure: Interview DAA and IAO. Review written policies and training material. Request IAO demonstrate these configuration settings by sample checking a few PDA devices.	3.4.5.2

Comments:
WIR0480 / CAT III / 1-CS / 2-CS / 3-CS / ECCD-1, ECCD-2, ECCR-1, ECCR-2, ECCR-3 **PDI Short Description**: PDA hotsyncing procedures for unclassified information are not followed or do not exist.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0490 For PDA access via Internet, use encryption, PKI and turn off modem when not in use

O	NF	NR	NA	Policy	STIG Reference
				If the PDA is used for wireless Internet remote access to DoD networks, the following applies: - The IAO will ensure that data encryption meeting the FIPS 140-2 (3DES or AES) standard will be used on the PDA. - The IAO will ensure that DoD PKI certificates will be used for identification and authentication of users. (Waived if PKI certificates are not being used by agency.) - The IAO will ensure that PDA wireless modems (e.g. IEEE 802.11, cellular, etc.) are removed or turned off when wireless data connections are not being used. Procedure: Review site policy and PDA configuration documents. Work with the SA or IAO to verify that all PDAs used to process government data use encryption to protect data stored on the device. Third party or Palm or Windows OS. Verify FIPS certified products by reviewing the IAO provided certificate.	3.4.5.2

WIR0490 / CAT II /
PDI Short Description: PDA accessing remotely via Internet do not use encryption, PKI, or modem remains on when not in used.

Open		Not a Finding		Not Reviewed		Not Applicable	

4.3.2 Mitigating Risks to Classified Information

WIR0380 Use NSA Type 1 end-to-end encryption classified PDAs

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that PDA used to transfer, receive, store, or process classified data will use NSA approved, Type 1 end-to-end encryption for data being transferred, received, stored or processed. **Note**: PDA must be handled in accordance with applicable regulations at the level of the classified data stored or processed on the device. Procedure: Request IAO demonstrate the configuration or use of file encryption on the PDA. Verify encryption method used has NSA certification at the classification level of the data stored on the device. **Hints:** Currently, there are no NSA approved Type-1 devices for PDAs. Approved devices are not expected to be available until late 2005.	3.4.5.1

Comments:

WIR0380 / CAT II /
PDI Short Description: PDAs that process classified information are not using NSA-approved, Type 1 end-to-end encryption.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0390 Disable RF and IR on PDAs if permitted in SCIFs

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that PDAs are not permitted in a permanent, temporary, or mobile SCIF unless the transmit capability (RF and IR) is rendered inoperable. **Note**: Taping is not sufficient. User must remove or disable card and/or disable port on the device. It is not possible to disabling the IR port on a PDA, care should be taken to procure PDAs without these ports or the DAA should not allow into SCIFs. Procedure: Interview the IAO and request copies of the security briefing to verify that personnel have been properly instructed in the requirement.	3.4.5.1

Comments:

WIR0390 / CAT II /
PDI Short Description: PDAs are permitted in a SCIF without the RF or IR disabled.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0400 For PDAs used where classified is processed, coordinate with CTTA and disable recording

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that PDAs are permitted in an area where classified data is discussed or processed only when: - The DAA, in consultation with the CTTA, has approved that PDAs can be brought into the facility and/or used in the facility. - The PDAs are separated from the classified data equipment a distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented. - The device’s voice recording capability is rendered inoperable. Procedure: Review documentation showing CTTA coordination. Note specific areas identified as approved or prohibited for wireless device use. Review written policies and training material. Verify that the voice recording is not enabled. Verify proper procedures for wireless device use in classified areas is addressed in training program.	3.4.5.1

Comments:							
WIR0400 / CAT II / **PDI Short Description:** PDAs are used in unauthorized areas or do not have proper approval for use in these areas.							
Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0410 Do not connect PDA directly to classified workstations or in classified areas

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that users do not connect PDAs directly to workstations transferring, receiving, storing, or processing classified data in a SCIF or other classified areas. Procedure: Interview DAA and IAO. Review written policies and training material. Review any devices, which are identified as used in these location and note if the IR/IF ports on the PDA is disabled using hardware or software.	3.4.5.1

Comments:							
WIR0410 / CAT II / **PDI Short Description:** PDAs are not prohibited from directly connecting to workstations located in classified areas.							
Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0420 Do not hotsync to or install PDA synchronization software on workstations in a SCIF

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that synchronization software will not be loaded on systems processing classified information. Classified information will not be synched. PDAs will not be connected via hotsync to a workstation in a SCIF. Procedure: Interview DAA and IAO. Review written policies and user agreement or training material. Reviewer may also physically check for synchronization cable on device or docking station.	3.4.5.1

Comments:

WIR0420 / CAT II /
PDI Short Description: PDA synchronization software is loaded on systems processing classified information or are allowed to connect via hotsync to workstations in a SCIF

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0425 Encrypt classified data on PDA using NSA approved encryption

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that classified data stored on PDA is encrypted using NSA approved encryption consistent with the classification level of the data stored on the device. Procedure: Interview the IAO and obtain documentation showing encryption used for wireless PDA devices used to store, process, or communicate with classified have FIPS compliant encryption. Mark this as a CAT II finding if FIPS compliant encryption is not used.	3.4.5.1

Comments:

WIR0425 / CAT II /
PDI Short Description: Classified data on PDA is encrypted using NSA approved encryption.

Open		Not a Finding		Not Reviewed		Not Applicable	

This page intentionally left blank.

5. WIRELESS TWO-WAY MESSAGING AN

6. D E-MAIL TECHNOLOGIES

6.1 Mitigating Risks to Classified Information

WIR0500 Do not use wireless messaging devices to process classified

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that wireless messaging devices, will not be used to send, receive, store, or process classified messages. Procedure: Interview DAA and IAO. Review written policies and training material.	4.2.3.1 4.3.1.1 4.4.3.1

Comments:
WIR0500 / CAT III / **PDI Short Description:** Wireless messaging devices are used to send, receive, store, or process classified information.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0510 Disable RF and IR for wireless messaging devices if permitted in a SCIF

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that wireless messaging devices are not permitted in a permanent, temporary, or mobile SCIF unless the transmit capability (RF and IR) is rendered inoperable. Procedure: Review written policies and training material. Powering off is not necessarily effective for all models. Removal of batteries is a more acceptable procedure.	4.2.3.1 4.3.1.1 4.4.3.1

Comments:
WIR0510 / CAT III / **PDI Short Description:** Wireless messaging devices are permitted in SCIFs without the RF or IR capabilities rendered inoperable.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0520 Coordinate with CTTA for SMS/pagers before entering classified processing areas

O	NF	NR	NA	Policy	STIG Reference
			3	The IAO will ensure that wireless messaging devices are not permitted in an area where classified data processing takes place unless: - The DAA, in consultation with the CTTA, has approved the SMS device to enter into and or be used in the facility. - The SMS device is separated from the classified data equipment at a distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented. Procedure: Review documentation showing CTTA coordination. Note specific areas identified as approved or prohibited for wireless device use. Review written policies and training material. Verify proper procedures for wireless device use in classified areas is addressed in training program.	4.2.3.1 4.3.1.1 4.4.3.1

Comments:

WIR0520 / CAT III /
PDI Short Description: Wireless messaging devices process classified data or are used in unauthorized areas.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0530 Do not install synchronization software on systems processing classified information

O	NF	NR	NA	Policy	STIG Reference
			4	The IAO will ensure that synchronization software will not be loaded on systems processing classified information. Procedure: Interview DAA and IAO. Review written policies and training material. Reviewer may also check for synchronization cables on device, docking station, or syncing station, which may be attached to workstations used to process classified.	4.4.3.1

Comments:

WIR0530 / CAT II /
PDI Short Description: Synchronization software is loaded on systems processing classified information.

Open		Not a Finding		Not Reviewed		Not Applicable	

6.2 Compliance Checks for Wireless Messaging Devices

WIR0540 Use SMS and two-way pagers for routine administrative information only

O	NF	NR	NA	Policy	STIG Reference
			1	The IAO will ensure that SMS and two-way pagers will be used to send and receive unclassified routine/administrative information only. Procedure: Interview DAA and IAO. Review written policies and training material.	4.2.3.2 4.3.1.2 4.4.3.2

Comments:							
WIR0540 / CAT III / **PDI Short Description:** Wireless messaging devices are used for purposes other than routine administrative information.							
Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0550 Use messaging services that provide link encryption for SMS and two-way pagers

O	NF	NR	NA	Policy	STIG Reference
			2	The IAO will ensure that wireless messaging services (SMS and two-way pagers) provide data encryption for the wireless link. Procedure: Interview the IAO and obtain documentation showing encryption is provided over the wireless link by the service provider. Encryption does not have to be FIPS Compliant.	4.2.3.2 4.3.1.2 4.4.3.2

Comments:							
WIR0550 / CAT III / **PDI Short Description:** Wireless messaging services do not provide data encryption.							
Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0580 Configure password protection IAW DISA requirements

O	NF	NR	NA	Policy	STIG Reference
			3	The IAO will ensure that password protection, where a password must be entered in order to access device data and applications, will be used on all SMS, two-way paging, and two-way email devices. - If possible, a password meeting DoD password policies will be used**.** - The password will be changed at least every 90 days. - If used, the password protection feature will not permit its bypass without zeroing all data stored on the device. - The password protection feature will be enabled. Procedure: Review site password policy and training with IAO. Ensure policy and password section of security training addresses each device used.	4.2.3.2 4.3.1.2 4.4.3.2

Comments:
WIR0580 / CAT I / 1-CS / 2-CS / 3-CS / ECCD-1, ECCD-2, ECCR-1, ECCR-2, ECCR-3 **PDI Short Description:** Password protection is not used or permits bypass without zeroing out data.

Open		Not a Finding		Not Reviewed		Not Applicable	

6.2.1 BlackBerry Email Devices

WIR0590 Use only BlackBerry enterprise server email redirectors

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that only the BlackBerry enterprise server email redirector is used. **Note:** Workstation based redirectors will not be used for wireless email systems. Procedure: Interview IAO. Review configuration of BlackBerry enterprise server to verify compliance.	4.4.3.2

Comments:
WIR0590 / CAT II/ **PDI Short Description:** Redirectors other than the BlackBerry enterprise server email redirector are used.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0600 Encrypt data and files on the BlackBerry device

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that tools are used to encrypt data and files on the BlackBerry device. Procedure: Interview IAO and review configuration documentation and policies for BlackBerry devices. Encryption comes with the BlackBerry and is on by default.	4.4.3.2

Comments:
WIR0600 / CAT II/ **PDI Short Description:** Files on BlackBerry devices are not encrypted

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0605 Download mobile code from DoD sources only

O	NF	NR	NA	Policy	STIG Reference
				Mobile code will not be downloaded from non-DoD sources and will be downloaded from only trusted DoD sources over assured channels. Procedure: Review site policy and training with IAO. Interview users to ensure they are aware and comply with this requirement.	4.4.3.2

Comments:
WIR0605 / CAT II/ **PDI Short Description:** Mobile code is downloaded from non-DoD sources.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0610 Disable BlackBerry IR port when not in use; exchange data with trusted devices only

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that the BlackBerry device IR port is disabled when IR transmissions are not being used. Data exchange via the IR port should be limited to only trusted DoD devices. Procedure: Review **written** policy and check configuration of BlackBerry devices if possible. Not all models of BlackBerries have an IR port. Mark this as a finding if policy documents are not available or if users are not trained on this requirement.	4.4.3.2

Comments:
WIR0610 / CAT II/ **PDI Short Description:** IR ports of BlackBerry devices are not disabled when not in use or allow data exchange with untrusted devices.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0620 Deactivate BlackBerry devices at the server when reported lost or stolen

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that a BlackBerry device is deactivated at the BlackBerry server if it is reported lost or stolen. Procedure: Review written policies and end user training materials to verify compliance. Verify that proper procedures are followed when devices are lost or stolen. If a BlackBerry device is lost or stolen, the device must be immediately disabled to prevent unauthorized use or access. Once the device has been determined to be unrecoverable, the device should be permanently removed from the server and SA should contact the service provider to cancel the service.	4.4.3.2

Comments:
WIR0620 / CAT III/ **PDI Short Description:** BlackBerry devices are not deactivated at the BlackBerry server when the device is lost or stolen.

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0630 Blackberry password protection must comply with DISA policy

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that password protection, where a password must be entered in order to access device data and applications, is used. - A password meeting DOD password policies will be used and the password will be changed at least every 90 days. - The password protection feature will not permit its bypass without zeroing all data stored on the device. (default setting) - The password protection feature will be enabled at all times. Procedure: Review site password policy and training with IAO. Verify policy and password section of security training addresses each device used.	4.4.3.2

Comments:

WIR0630 / CAT II/ 1-CS / 2-CS / 3-CS / ECCD-1, ECCD-2, ECCR-1, ECCR-2, ECCR-3
PDI Short Description: Blackberry password protection is not used or is not meet DISA policy.

Open		Not a Finding		Not Reviewed		Not Applicable	

This page intentionally left blank

APPENDIX A. CRITICAL LEVEL 1 CHECKS

All SRR teams are required to check out a wireless discovery tool prior to departing for the site. This tool is used by a trained team member to perform wireless discovery test using the instructions outlined in the Wireless SCV documentation.

If **WLAN** access points and/or clients are discovered or identified by the site during the SRR, the appropriate sections of the Wireless checklist will be completed or a Wireless SRR will be scheduled if time or resources does not permit. If all checks in Section 1 and Section 2 cannot be performed, then the following checks are the most critical for immediate mitigation of network level security risks and are intended to minimally secure the wireless environment while allowing time for a complete Wireless SRR to be scheduled.

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that all wireless systems are approved by the DAA prior to installation and use for processing DoD information **Note:** The Level 1 Check applies to WLAN devices only (i.e. access points, routers, bridges, switches, IDS's, firewall, and laptops) Procedure: To save time on site, and help facilitate the SRR, prior to arrival at the site, complete the Wireless Inventory Sheet and use this information to research FIPS 140-2 compliance for devices identified. Request a copy of the sites wireless equipment inventory list, which is required in PDI WIR0015. Also, request an electronic copy of the SSAA and DAA/CTTA approval documentation for review. Use the inventory list and approval documents to note specific products by model, specifications, location restrictions, classification levels, etc. for which approval was granted. Finally, verify DAA approval for each product includes wireless services, accessories, operating systems, and applications used with each wireless device. Verify the mission need is still valid and the approval applies to the specific wireless devices and configurations in use.	**Level 1 Check** 2.1 2.2.6.1

Comments:

WIR0010 / CAT III / 1-CSP, 2-CSP, 3-CSP / DCPR-1, DCHW-1, DCSW-1
PDI Short Description: A wireless system does not have DAA approval.

Open		Not a Finding		Not Reviewed		Not Applicable

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that WLAN devices are not used to transfer, receive, store, or process classified information categorized as SCI and TS. Procedure: Interview the IAO and request copies of the security briefing to verify that personnel have been properly instructed in the requirement. Mark this as a finding if WLAN devices are used for classified information or SCI level traffic.	**Level 1 Check** 2.2.6.1

Comments:

WIR0170 / CAT II / 1-C / 2-C / 3-C / DCSR-3, ECWN-1
PDI Short Description: WLAN devices are used to access TS and SCI information.

Open		Not a Finding		Not Reviewed		Not Applicable	

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that WLANs and WPANs are not operated in areas where classified information is electronically stored, processed, or transmitted unless: - The DAA, in consultation with the CTTA, has approved the use of WLANs or WPANs (such as Bluetooth) devices in the area. - The device's voice recording capability is rendered inoperable. - The WLAN is separated from the classified data equipment by a distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented. Procedure: Review documentation showing CTTA notification and review of the system. Note specific areas identified as approved or prohibited for wireless device use. Document must also specify distance and countermeasure guidelines. Mark this PDI as a finding if written CTTA coordination does not exist for all systems which process or transmit classified data.	**Level 1 Check** 2.2.6.1 2.3.1.1

Comments:

WIR0225 / CAT II / 1-C / 2-C / 3-C / ECTC-1
PDI Short Description: WLAN devices are used or installed in unauthorized areas.

Open		Not a Finding		Not Reviewed		Not Applicable	

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that MAC address filtering is enabled at each access point. **Note**: MAC address filtering may not be practical for large WLAN implementations, unless the WLAN management system allows for MAC distribution lists to be centralized and automatically distributed to the point of authentication. Procedure: Review the configuration of the WLAN access point to check for compliance. If the WLAN supports joint operation in a deployed environment, then this PDI may be marked as not applicable.	**Level 1 Check** 2.2.3.2 2.2.6.2

Comments:
WIR0160 / CAT II / 1-CSP / 2-CSP / 3-CSP / ECWN-1 **PDI Short Description:** MAC address filtering is not enabled on all access points.

Open		Not a Finding		Not Reviewed		Not Applicable	

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that the wireless LAN provides a session timeout capability and the timeout is set for 15 minutes or less depending on local security policy Procedures: Review the configuration of the wireless security gateway (e.g. VPN) appliance or other applicable network device to ensure session timeout is set for 15 minutes or less. (Normally, this is not in the access point configuration but is set in the wireless security gateway). This setting can sometimes also be set in the AP but this is not the best method of implementation.	**Level 1 Check** 2.2.6.2

Comments:
WIR0230 / CAT II / 1-CSP / 2-CSP / 3-CSP / ECND-1, ECND-2, ECTM-2, ECWN-1 **PDI Short Description:** WLAN session timeout is not set to 15 minutes.

Open		Not a Finding		Not Reviewed		Not Applicable	

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that the WLAN access point is set to the lowest possible transmit power setting that will meet the required signal strength of the area serviced by the access point. Procedure: Interview IAO and request documentation showing signal strength analysis from site survey activities. If available, use testing equipment or WLAN clients to determine if signal strength is, in the reviewer judgment, excessively outside the required area. Lower end APs will not have this setting available—in this case, the site should locate the APs appropriately to achieve compliance with this requirement.	**Level 1 Check** 2.2.6.2

Comments:
WIR0250 / CAT II / 1-CSP / 2-CSP / 3-CSP / ECTM-2, ECWN-1 **PDI Short Description:** WLAN AP transmit power is not set to the lowest possible level to obtain required signal strength.

Open		Not a Finding		Not Reviewed		Not Applicable	

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that PKI certificates are used for identification and authentication of the user on unclassified WLAN systems. **Note:** This check applies only to unclassified systems. Perform WIR0210 in Section 2.4 for classified systems, which require high assurance PKI specifically. Procedure: Interview the IAO and verify use of DoD PKI certificates. Review written policies and training materials. If PKI is not yet implemented on DISANET for this site, so state and mark as "not a finding".	**Level 1 Check** 2.2.6.2

Comments:
WIR0240 / CAT II / 1-S / 2-S / 3-S / IAIA-1, DCBP-1 **PDI Short Description:** Unclassified WLAN does not use DoD PKI certificates.

Open		Not a Finding		Not Reviewed		Not Applicable	

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure WLAN network devices, such as access points and bridges, are placed in a screened subnet (DMZ) or Virtual LAN (VLAN) and separated from the wired internal network. A VPN concentrator or gateway will be placed between the access point and the local DoD network. Procedure: Verify compliance by inspecting the site network topology diagrams and the firewall interface configurations. Since many network diagrams are not kept up-to-date, have network administrator walk through the connections to verify the accuracy of the diagrams.	**Level 1 Check** 2.2.6.2 2.2.2.2.2

Comments:

WIR0290 / CAT II / 1-SP / 2-SP / 3-SP / EBBD-1, EBBD-2, EBBD-3, EBVC-1, ECWN-1
PDI Short Description: WLAN access points and bridges are not installed in an isolated subnet.

Open		Not a Finding		Not Reviewed		Not Applicable	

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure an Intrusion Detection System (IDS) (network IDS/IPS or wireless IDS/IPS) is used to monitor the wireless network. Procedure: Interview network administrator and verify compliance by inspecting the site network topology and dataflow diagrams. To comply with this requirement, the site may either place an IDS/IPS sensor on the wired portion of the network or use a wireless IDS//IPS.	**Level 1 Check** 2.2.6.2

Comments:

WIR0300 / CAT II / 1-CSP / 2-CSP /3-CSP / ECID-1, EBVC-1
PDI Short Description: An IDS/IPS is not used to monitor the wireless network.

Open		Not a Finding		Not Reviewed		Not Applicable	

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure HTTP, SNMP and other management interfaces on wireless access points and bridges will be turned off after initial configuration. These ports will be turned on only for firmware upgrades as needed. **Note:** If this feature is not available on the device, then the port should be protected using strong, two-factor authentication/password. Procedure: Review access point configuration to see if HTTP and SNMP ports are turned off. Ports may be turned on for limited time for firmware updates but must be turned off after use (per Network Infrastructure Security STIG). Do not mark as a finding if this capability is not available on the lower end device but risk is mitigated though use of password protection is used on the port.	**Level 1 Check** 2.2.2.2.2 2.2.6.2

Comments:

WIR0320 / CAT II / 1-CSP, 2-CSP, 3-CSP / DCPP-1
PDI Short Description: WLAN network management ports remain enabled when not in use.

Open		Not a Finding		Not Reviewed		Not Applicable	

O	NF	NR	NA	Policy	STIG Reference
				The IAO will ensure that a password is required for access to the management console for the WLAN access point or WLAN bridging device and that the password complies with DoD password policies. Procedure: Review access point configuration to see if password access is enabled for access to the management and configuration settings. Mark this PDI as a finding if password access to the management console is not enabled.	**Level 1 Check** 2.2.6.2 2.2.2.2.2

Comments:

WIR0330 / CAT I / 1-SP / 2-SP / 3-SP / ECND-1, ECND-2, ECPA-1, IAIA-1
PDI Short Description: WLAN communications devices are not password protected in accordance with DISA requirements.

Open		Not a Finding		Not Reviewed		Not Applicable	

APPENDIX B DISABLING WINDOWS WIRELESS ZERO CONFIGURATION (WZC)

The following procedures apply to both the Windows 2000 and the Windows XP WLAN clients.

If the Windows Services snap-in is installed (preferred method):

1. Right click Start, then Control Panel, then Performance and Maintenance, then Administrative Tools, and then double click Services.
2. Double click on the Wireless Zero Configuration icon.
3. Select the General tab.
4. Under Startup Type select Disabled.
5. Under Service Status, ensure the status is set to Stopped.
6. Click OK and close the Services screen.

If the Windows Services snap-in is not installed:

Note: This procedure will only work if the installed wireless adapter supports the Windows WZC service. If the wireless adapter does not support the WZC service, no action is needed. You must be logged as a user with administrator rights.

1. Right click Start, then Control Panel, then Network and Internet Connections, and then Network Connections
2. Right click Wireless Network Connection, then Properties
3. On the Wireless Networks tab, clear the Use Windows to Configure My Wireless Network check box.

APPENDIX C WIRELESS PRODUCT LISTS

The following is a list of tools that may help the site and the reviewer when performing wireless assessments. The information in this section does not automatically imply DISA approval (wholly or in part) of these products. These references have been requested by our users to server as a starting point for researching wireless hardware and software. Verify each product version if still compliant by appropriate documentation from vendor prior to purchase of product. This list will be updated monthly, or as new products are brought to our attention.

DoD Community of Practice Knowledge Management Web Site

http://acc.dau.mil
Select the "DoD Wireless" community and follow the instructions to register.

PDA Antivirus Products

A current list of approved antivirus products is located on the DISA antivirus web site.
http://www.cert.mil

PDA Firewalls/Security Products

The following products use or can be configured to use data encryption that is FIPS 140-2 compliant. Verify each product model by requesting FIPS compliance documentation from vendor prior to purchase of product.

- Bluefire Security Technologies "Bluefire Mobile Firewall" and "Bluefire Mobile Firewall Plus"
- Credant Technologies Corp. "CREDANT Mobile Guardian"
- Pointsec (Various products are available)
- Certicom Corp. "movianVPN GSE" and "movianCrypt GSE"

Tools to Disable Bluetooth on Laptops

This list may not be current. Verify each product model prior to purchase.

- Bluefire Security Technologies "Bluefire Mobile Firewall" and "Bluefire Mobile Firewall Plus"
- Credant Technologies Corp. "CREDANT Mobile Guardian"

Type 1 Certified Cell Phones

http://www.securephone.net/

FIPS 140-2 Certified WLAN Security Gateways

This list may not be current. Verify each product model by requesting FIPS compliance documentation from vendor prior to purchase of product.

- Fortress technologies “AirFortress” (Several models available)
- Cranite Systems, Inc. “Wireless Wall”
- Airspace, Inc. (Several products available)
- 3e Technologies International, Inc. (Several models available)
- Reefedge, Inc. (Several models available)
- Symbol (Columbitech) “AirBeam Safe”

FIPS 140-2 Certified WLAN IDS

This list may not be current. Verify each product model by requesting FIPS compliance documentation from vendor prior to purchase of product.

- Air Defense WIDS

This page is intentionally left blank.